RECEIVED
CENTRAL FAX CENTER
AUG 17 2006

Remarks

Reconsideration of the above-captioned application is respectfully requested. Claims 1-6, 8-12, 14-18, and 20-23, of which Claims 1, 8, 14, and 20 are independent, have been rejected under 35 U.S.C. §102 as being anticipated by Wheeler et al., USPP 2003/0097569 and by Wheeler et al., USPN 6,915,430 which is the issued patent of the Wheeler publication. Claims 1-24 have also been rejected under 35 U.S.C. §102 as being anticipated by the TCG specification, while dependent Claims 7, 13, 19, and 20 have been rejected under 35 U.S.C. §103 as being unpatentable over Wheeler '430 in view of TCG.

The fact that Applicant has focussed its comments distinguishing the present claims from the applied references and countering certain rejections must not be construed as acquiescence in other portions of rejections not specifically addressed.

To overcome the Examiner's rejections, Claim 1 has been amended to specify erasing the temporary secret from the security module after the certificate request data has been sent to the comparison agent so that the temporary secret cannot subsequently be discovered as disclosed on page 6, line 15. Independent Claim 8 now recites that the nonce is erased from the security module after the data representative of the public key has been sent to the source so that the nonce cannot subsequently be discovered. Independent Claim 14 as amended sets forth that the data representative of a public key includes a hash of the public key and a secret, with the secret being erased from the customer computing device after the data representative of the public key has been sent to the facility such that the secret cannot be rediscovered. Independent Claim 20 as now amended requires that the data representative of a public key includes a hash of the public key and a secret, and the secret is erased from a customer computing device after the data representative of the public key has

PAGE 7/10 * RCVD AT 8/17/2006 5:03:33 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:16193388078 * DURATION (mm-ss):01-58

been sent to the facility so that the secret cannot be rediscovered. Claims 1-6, 8-11, 14-17, and 20-22 remain pending.

Rejections Under 35 U.S.C. §102

Claims 1-6, 8-12, 14-18, and 20-23, of which Claims 1, 8, 14, and 20 are independent, have been rejected under 35 U.S.C. §102 as being anticipated by Wheeler et al., USPP 2003/0097569 and by Wheeler et al., USPN 6,915,430 which is the issued patent of the Wheeler publication. Claims 1-24 have also been rejected under 35 U.S.C. §102 as being anticipated by the TCG specification.

As admitted in the Office Action, Wheeler et al does not teach erasing a nonce or secret after use, so this reference will not be further discussed in this section. This leaves the TCG specification, which is addressed in the present background. With this fact in mind it is not surprising that the rejections erroneously find anticipation in TCG.

With more specificity, page 306 of TCG has been relied on as the claimed "request for a certificate", but all this portion teaches appears to be that a public key is concatenated with an ID and then hashed using SHA, not that it constitutes a request for a certificate. Furthermore, page 303 has been relied on as the claimed content of the certificate request, but this page is neither linked to the subject matter relied on at page 306 as the alleged certificate request nor does it say anything itself about certificate requests. Instead, it appears to teach that interoperability among devices is achieved by providing a set of algorithms and message formats that devices may select from. And, since the ensuing portions of TCG relied on for claim limitations that follow those discussed above precede pages 303 and 306 in TCG, the elements for which they have been relied cannot flow from the certificate request in the way claimed.

PAGE 8/10 * RCVD AT 8/17/2006 5:03:33 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:16193388078 * DURATION (mm-ss):01-58

Rejections Under 35 U.S.C. §103

Claims 7, 13, 19, and 20 have been rejected under 35 U.S.C. §103 as being unpatentable over Wheeler '430 in view of TCG, page 14, section 3.1, last paragraph, which, as correctly noted in the Office Action, teaches erasing data only after it has been converted to another data structure and, hence, can be rediscovered, in contrast to the present claims. As envisioned by the present invention but not the combined references, a one time-only request for a certificate can thus be provided for. Accordingly, since it does not appear that the references suggest this feature, the claims are patentable.

Applicant would also like to point out that in Wheeler et al., as taught in column 7 the relied-upon public key is not hashed with a temporary secret, much less one that is later erased. Instead, Wheeler et al., which is directed to linking a security profile to a public key so that a user can determine the level of security of the associated module, provides a certificate by linking the public key to a security profile which is then signed by a digital signature to render the certificate, and the Office Action does not establish that a digital signature is a temporary secret.

The Examiner is cordially invited to telephone the undersigned at (619) 338-8075 for any reason which would advance the instant application to allowance.

Respectfully submitted,

John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1191-2.AMD